ECSAV8Q&As

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL ECSAV8 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

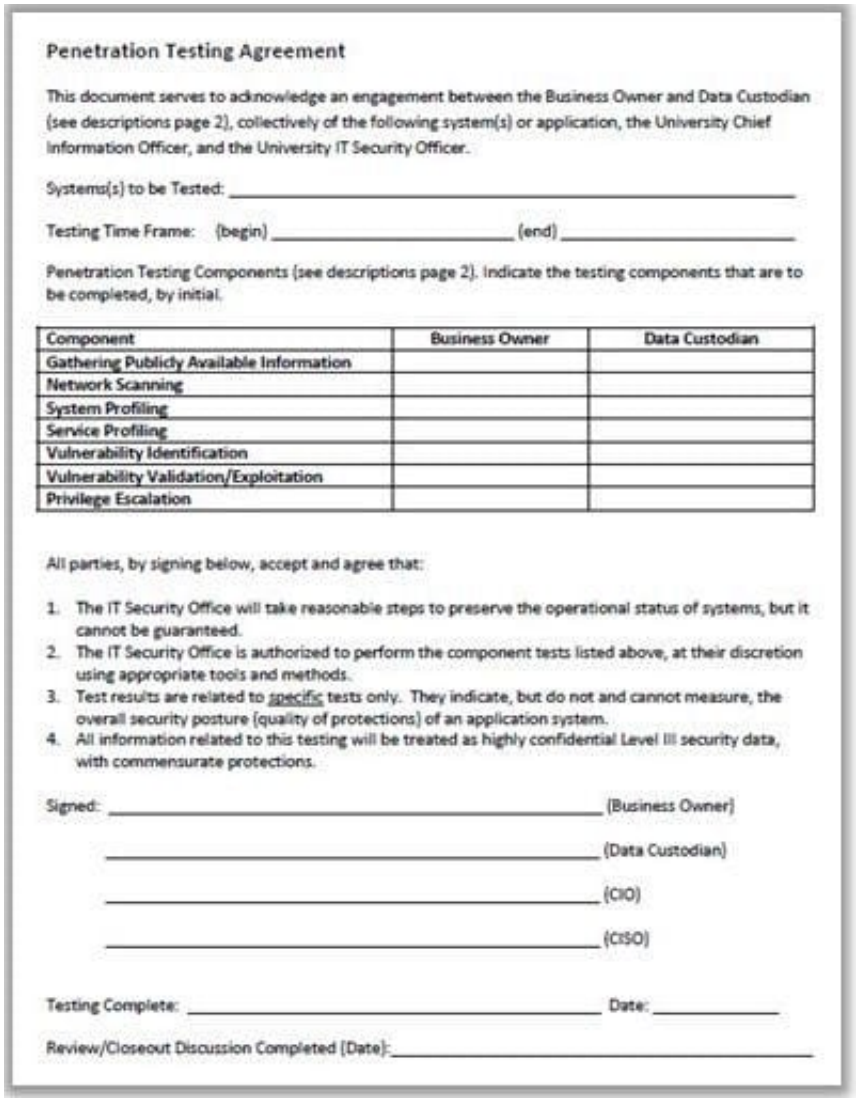
https://www.leads4pass.com/ecsav8.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Why is a legal agreement important to have before launching a penetration test?



Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be Tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: _____ (Business Owner)

_____ (Data Custodian)

_____ (CIO)

_____ (CISO)

Testing Complete: _____ Date: _____

Review/Closeout Discussion Completed (Date): _____

A. Guarantees your consultant fees

B. Allows you to perform a penetration test without the knowledge and consent of the organization\\'s upper management

C. It establishes the legality of the penetration test by documenting the scope of the project and the consent of the company.

D. It is important to ensure that the target organization has implemented mandatory security policies

Correct Answer: C

QUESTION 2

Which of the following attacks does a hacker perform in order to obtain UDDI information such as businessEntity, businesService, bindingTemplate, and tModel?

A. Web Services Footprinting Attack

B. Service Level Configuration Attacks

C. URL Tampering Attacks

D. Inside Attacks

Correct Answer: A

Reference: http://www.scribd.com/doc/184891017/CEHv8-Module-13-Hacking-Web- Applications-pdf (page 99)

QUESTION 3

Which among the following information is not furnished by the Rules of Engagement (ROE) document?

A. Techniques for data collection from systems upon termination of the test

B. Techniques for data exclusion from systems upon termination of the test

C. Details on how data should be transmitted during and after the test

D. Details on how organizational data is treated throughout and after the test

Correct Answer: D

QUESTION 4

Identify the data security measure which defines a principle or state that ensures that an action or transaction cannot be denied.

A. Availability

B. Integrity

C. Authorization

D. Non-Repudiation

Correct Answer: D

Reference: http://en.wikipedia.org/wiki/Information_security (non-repudiation)

QUESTION 5

Which of the following has an offset field that specifies the length of the header and data?

A. IP Header

B. UDP Header

C. ICMP Header

D. TCP Header

Correct Answer: A

QUESTION 6

Which of the following appendices gives detailed lists of all the technical terms used in the report?

A. Required Work Efforts

B. References

C. Research

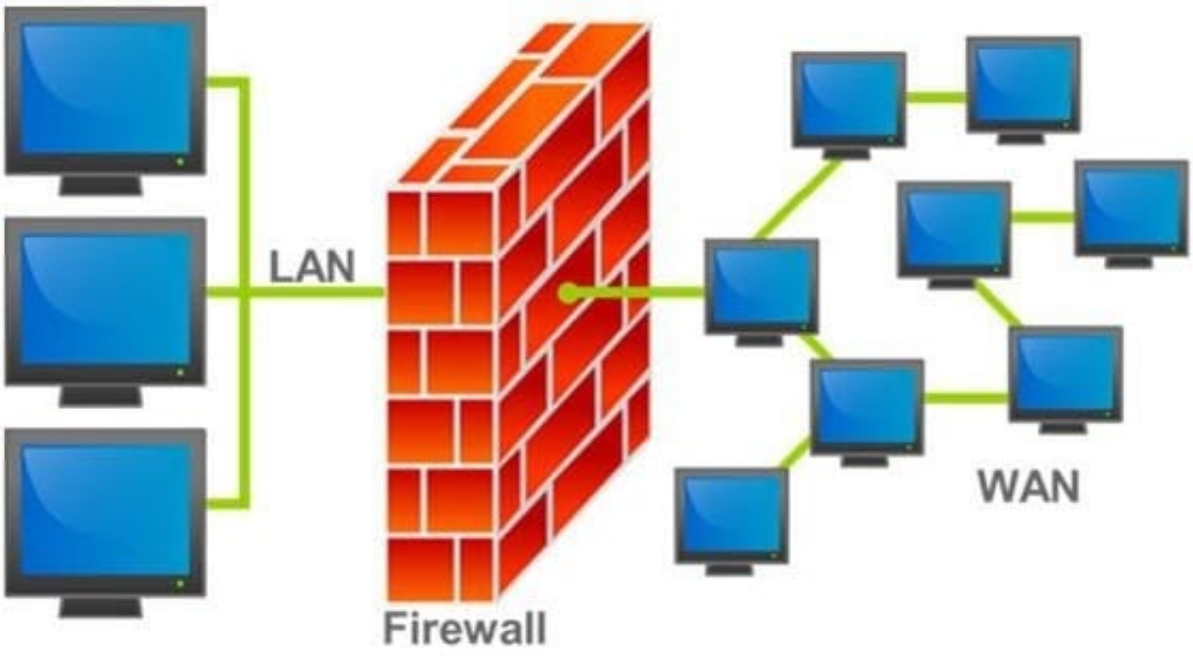
D. Glossary

Correct Answer: D

Explanation: Refere\\' http://en.wikipedia.org/wiki/Glossary

QUESTION 7

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped.



Why is an appliance-based firewall is more secure than those implemented on top of the commercial operating system

(Software based)?

A. Appliance based firewalls cannot be upgraded

B. Firewalls implemented on a hardware firewall are highly scalable

C. Hardware appliances does not suffer from security vulnerabilities associated with the underlying operating system

D. Operating system firewalls are highly configured

Correct Answer: C

QUESTION 8

The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations. Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.

What is the best way to protect web applications from parameter tampering attacks?

A. Validating some parameters of the web application

B. Minimizing the allowable length of parameters

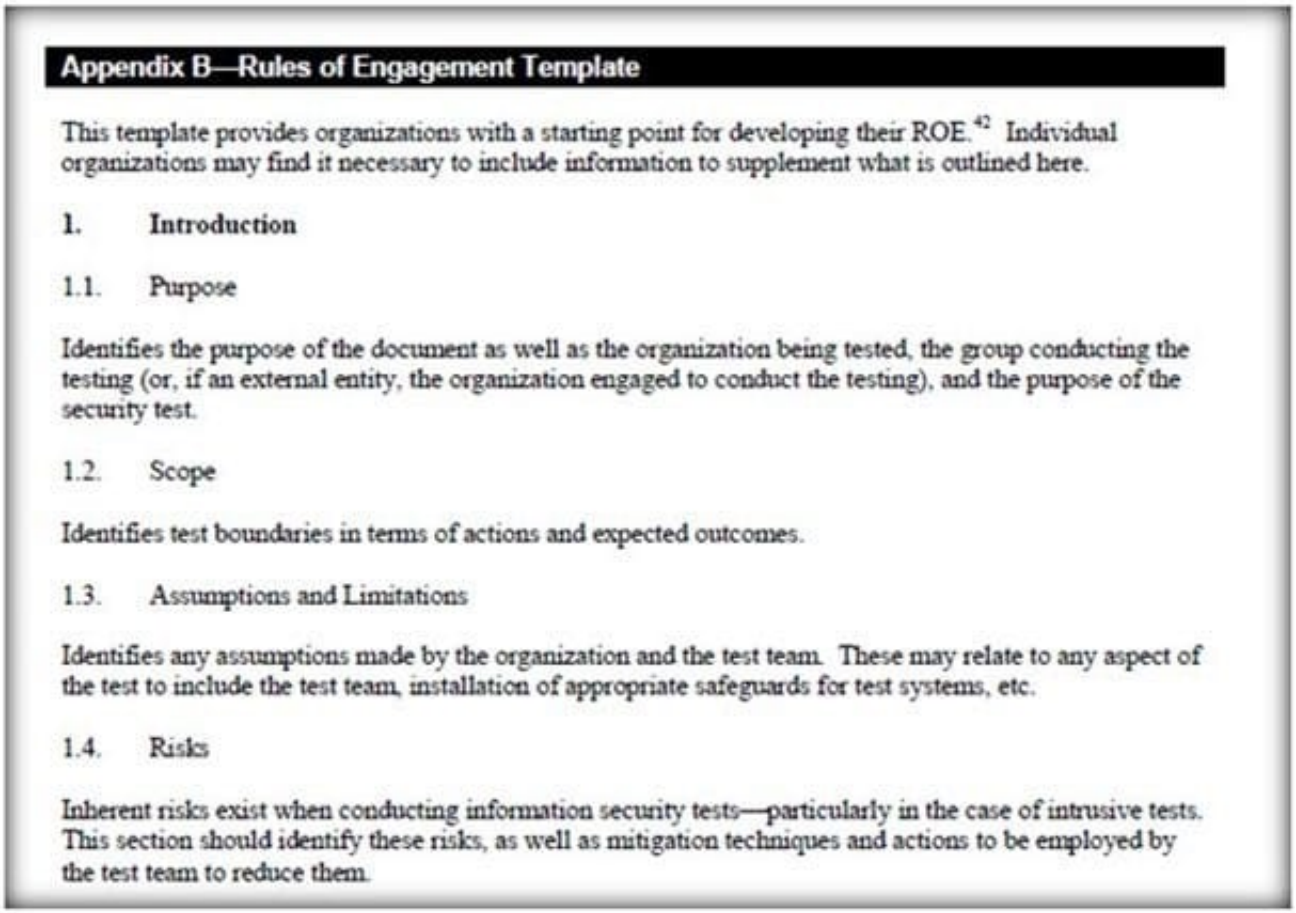
C. Using an easily guessable hashing algorithm

D. Applying effective input field filtering parameters

Correct Answer: B

QUESTION 9

Rule of Engagement (ROE) is the formal permission to conduct a pen-test. It provides top- level guidance for conducting the penetration testing. Various factors are considered while preparing the scope of ROE which clearly explain the limits associated with the security test.



Appendix B—Rules of Engagement Template

This template provides organizations with a starting point for developing their ROE.[42] Individual organizations may find it necessary to include information to supplement what is outlined here.

1. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (or, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, installation of appropriate safeguards for test systems, etc.

1.4. Risks

Inherent risks exist when conducting information security tests—particularly in the case of intrusive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

Which of the following factors is NOT considered while preparing the scope of the Rules of Engagment (ROE)?

A. A list of employees in the client organization

B. A list of acceptable testing techniques

C. Specific IP addresses/ranges to be tested

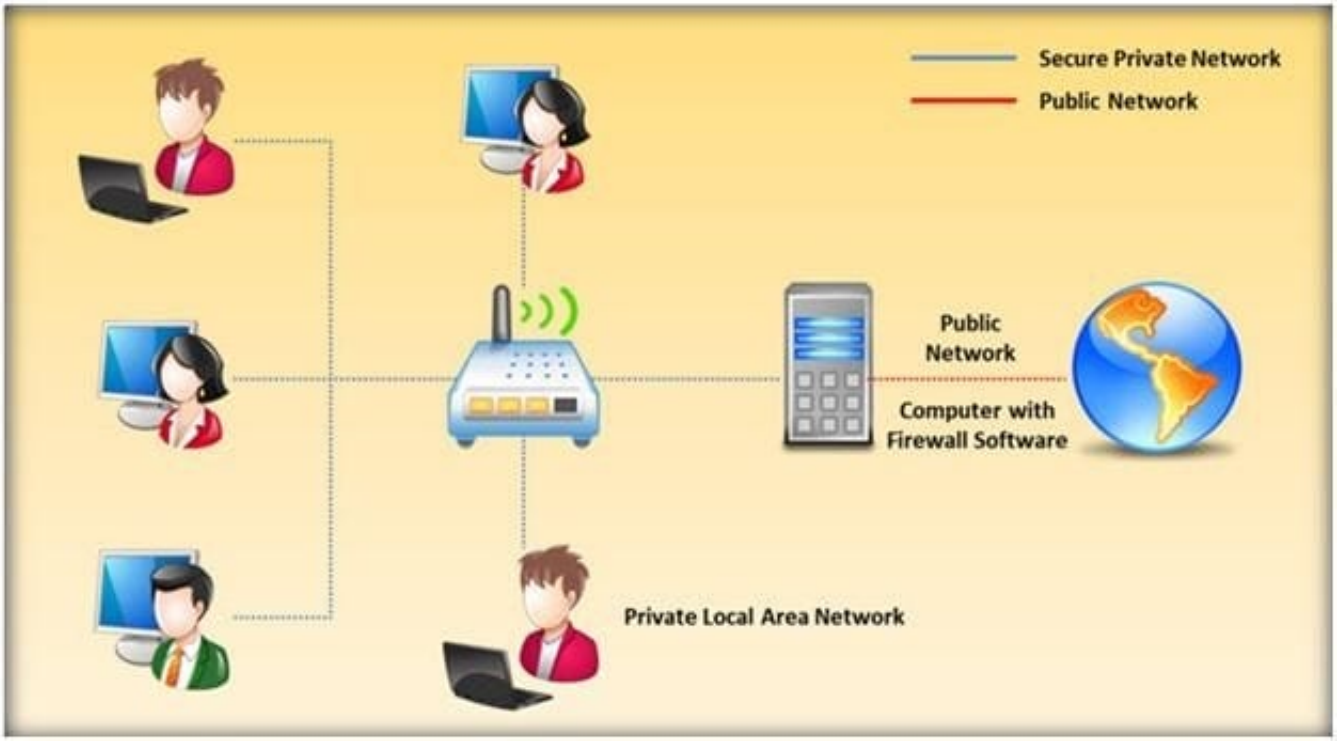
D. Points of contact for the penetration testing team

Correct Answer: A

QUESTION 10

Packet filtering firewalls are usually a part of a router. In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded.

Depending on the packet and the criteria, the firewall can: i)Drop the packet ii)Forward it or send a message to the originator



At which level of the OSI model do the packet filtering firewalls work?

A. Application layer

B. Physical layer

C. Transport layer

D. Network layer

Correct Answer: D

Reference:

http://books.google.com.pk/books?id=KPjLAyA7HgoCandpg=PA208andlpg=PA208anddq=At+whi ch+level+of

+the+OSI+model+do+the+packet+filtering+firewalls+workandsource=blandots=zRrb cmY3pjandsig=I3vuS3VA7r3VF8lC 6xq_c_r31Mandhl=enandsa=Xandei=wMcfVMetI8HPaNSRgPgDandved=0CC8Q6AEwAg#v

=onepageandq=At%20which%20level%20of%20the%20OSI%20model%20do%20the%20pa cket%

20filtering%20firewalls%20workandf=false (packet filters)

QUESTION 11

Which of the following protocols cannot be used to filter VoIP traffic?

A. Media Gateway Control Protocol (MGCP)

B. Real-time Transport Control Protocol (RTCP)

C. Session Description Protocol (SDP)

D. Real-Time Publish Subscribe (RTPS)

Correct Answer: D

QUESTION 12

Information gathering is performed to:

i) Collect basic information about the target company and its network

ii) Determine the operating system used, platforms running, web server versions, etc.

iii) Find vulnerabilities and exploits Which of the following pen testing tests yields information about a company\\'s technology infrastructure?

A. Searching for web page posting patterns

B. Analyzing the link popularity of the company\\'s website

C. Searching for trade association directories

D. Searching for a company\\'s job postings

Correct Answer: A

QUESTION 13

During the process of fingerprinting a web application environment, what do you need to do in order to analyze HTTP and HTTPS request headers and the HTML source code?

A. Examine Source of the Available Pages

B. Perform Web Spidering

C. Perform Banner Grabbing

D. Check the HTTP and HTML Processing by the Browser

Correct Answer: C

QUESTION 14

Which of the following is an ARP cache poisoning technique aimed at network switches?

A. Replay Attack

B. Mac Flooding

C. Man-in-the Middle Attack

D. DNS Poisoning

Correct Answer: B

Reference: http://www.watchguard.com/infocenter/editorial/135324.asp (see mac flooding)

QUESTION 15

SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the

data input or transmitted from the client (browser) to the web application.

A successful SQL injection attack can:

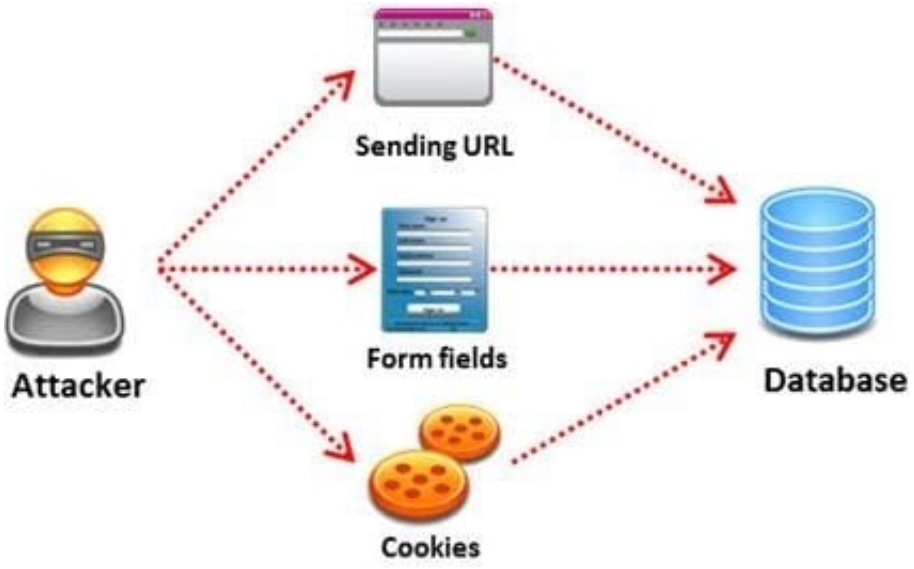
i)Read sensitive data from the database

iii)Modify database data (insert/update/delete)

iii)Execute administration operations on the database (such as shutdown the DBMS)

iV)Recover the content of a given file existing on the DBMS file system or write files into the file system

v)Issue commands to the operating system



Pen tester needs to perform various tests to detect SQL injection vulnerability. He has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate an error.

In which of the following tests is the source code of the application tested in a non-runtime environment to detect the SQL injection vulnerabilities?

A. Automated Testing

B. Function Testing

C. Dynamic Testing

D. Static Testing

Correct Answer: A

Reference:

http://ijritcc.org/IJRITCC%20Vol_2%20Issue_5/Removal%20of%20Data%20Vulnerabilities %20Using%

20SQL.pdf